



# Department of Defense DIRECTIVE

NUMBER 8100.2

---

---

ASD(NII)

SUBJECT: Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)

- References: (a) [DoD Directive 8100.1](#), "Global Information Grid (GIG) Overarching Policy," September 19, 2002
- (b) Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," November 18, 2002<sup>1</sup>
- (c) Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems," June 5, 1999<sup>1</sup>
- (d) [DoD Directive 8500.1](#), "Information Assurance (IA)," October 24, 2002
- (e) through (l), see enclosure 1

## 1. PURPOSE

This Directive:

1.1. Establishes the policy for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (reference (a)). Hereafter, the term "wireless" shall refer to commercial wireless.

1.2. Directs the development and use of a knowledge management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department.

---

<sup>1</sup> Limited Distribution. Contact the Office of the Intelligence Community Chief Information Officer.

1.3. Promotes joint interoperability using open standards throughout the Department of Defense for commercial wireless services, devices, and technological implementations.

## 2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. Applies to all DoD personnel, contractors, and visitors that enter DoD facilities or that have access to DoD information.

2.3. Applies to all commercial wireless devices, services, and technologies, including voice and data capabilities, that operate either as part of the DoD GIG, or as part of DoD non-GIG information technology (IT) (stand-alone) systems. This includes, but is not limited to: commercial wireless networks and portable electronic devices (PEDs), such as laptop computers with wireless capability, cellular/Personal Communications System (PCS) devices, audio/video recording devices, scanning devices, remote sensors, messaging devices, personal digital assistants (PDAs) and any other commercial wireless devices capable of storing, processing, or transmitting information.

2.4. Does not apply to information systems and/or Sensitive Compartmented Information Facilities (SCIF) to which DCID 6/9 (reference (b)) and DCID 6/3 (reference (c)) applies; i.e., Sensitive Compartmented Information and special access programs for intelligence under the purview of the Director of Central Intelligence (DCI).

2.5. Does not apply to receive-only pagers, Global Positioning System (GPS) receivers, hearing aids, pacemakers, other implanted medical devices, or personal life support systems. The detection segment of a PED (e.g., the laser beam between a laser disk and its reader head; between a barcode and a scanner head; or radio frequency (RF) energy between RF identification tags, both active and passive, and the reader/interrogator) does not require encryption.

### 3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

### 4. POLICY

It is DoD policy that:

4.1. Wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks, and must comply with DoD Directive 8500.1 (reference (d)) and be certified and accredited in accordance with DoD Instruction 5200.40 (reference (e)). In addition:

4.1.1. Strong authentication, non-repudiation, and personal identification is required for access to a DoD information system (IS) in accordance with the DoD public key infrastructure (PKI) policy established by DoD Chief Information Officer (CIO). Identification and Authentication (I&A) measures shall be implemented at both the device and network level. Voice does not require DoD PKI I&A.

4.1.2. Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the designated approving authority (DAA). At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-1 or FIPS PUB 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (references (f) and (g)). Encrypting unclassified voice is desirable. PEDs shall use file system encryption. Individual exceptions may be granted on a case-by-case basis as determined by the DAA.

4.1.3. Wireless devices shall not be used for storing, processing, or transmitting classified information without explicit written approval of the cognizant DAA. If approved by the DAA, only assured channels employing National Security Agency (NSA)-approved encryption shall be used to transmit classified information. Classified data stored on PEDs must be encrypted using NSA-approved encryption consistent with storage and treatment of classified information.

4.1.4. Measures shall be taken to mitigate denial of service attacks. These measures shall address not only threats from the outside, but potential interference from friendly sources.

4.1.5. Introduction of wireless technologies in DoD information systems, including those creating an external interface to non-DoD systems (or allowing use of DoD wireless devices on non-DoD wireless networks) can have a significant adverse effect on the security posture of the information system and requires security review and documentation in accordance with reference (d).

4.2. Cellular/PCS and/or other RF or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA).

4.3. Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA, in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

4.4. When unclassified wireless local area networks are used to support joint operations, Internet Protocol Security (IPSec) virtual private network technology shall be used and encrypted per subparagraph 4.1.2.

4.5. DAAs shall ensure that wireless personal area network capability is removed or physically disabled from a device unless FIPS PUB140-1/2-validated cryptographic modules are implemented (references (f) and (g)).

4.6. The DoD Components shall actively screen for wireless devices. Active electromagnetic sensing at DoD or contractor premises to detect/prevent unauthorized access of DoD information systems shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) ongoing accreditation agreement (reference (e)).

4.7. Mobile code shall not be downloaded from non-DoD sources. Downloading of mobile code shall only be allowed from trusted DoD sources over assured channels.

4.8. PEDs that are connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected.

4.9. Anti-virus software shall be used on wireless-capable PEDs and workstations that are used to synchronize/transmit data. The network infrastructure shall update anti-virus software for all applicable PEDs and their supporting desktops from a site maintained by the Defense Information Systems Agency.

4.10. The DoD Components shall seek and follow spectrum supportability guidance from the Military Communications-Electronics Board (MCEB) prior to assuming any contractual obligations for the full-scale development, production, procurement, or deployment of spectrum dependent (i.e., wireless) devices or systems, in accordance with DoD Directive 4650.1 (reference (h)).

4.11. A DoD wireless KM process shall be established. The goal is increased sharing of DoD wireless expertise to include information on vulnerability assessments, best practices, and procedures for wireless device configurations and connections.

4.11.1. The KM process shall be utilized by DAAs to help determine acceptable uses of wireless devices and employ appropriate mitigating actions.

4.11.2. DAAs shall submit alternative mitigating techniques for inclusion in the KM database. The DoD Components shall use the KM process to coordinate, prioritize, and avoid duplication of vulnerability assessments of wireless devices.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration, as the DoD Chief Information Officer, shall:

5.1.1. Monitor and provide oversight and policy development of all DoD wireless activities.

5.1.2. Establish a formal coordination process with the Intelligence Community (IC) CIO to ensure proper protection of IC information in implementing this Directive.

5.1.3. Ensure information interoperability of wireless capabilities in support of joint operations (references (i) and (j)).

5.1.4. Direct the development of acquisition strategies and assess potential architectures (e.g., wireless application frameworks) to minimize cost of wireless development, services and systems, achieve economies of scale, and promote

interoperability and security. As necessary, coordinate these activities with the Under Secretary of Defense for Acquisition, Technology, and Logistics.

5.1.5. Direct the development and implementation of a DoD wireless KM process to promote increased sharing of DoD wireless information.

5.1.6. Evaluate and approve specific implementation timelines for compliance of legacy systems to this Directive.

5.1.7. Ensure that the Director, Defense Information Systems Agency, shall:

5.1.7.1. Incorporate wireless considerations in its DoD-wide information assurance initiatives such as computer emergency response, vulnerability alerting, and enterprise anti-virus and file system/data store encryption software.

5.1.7.2. Provide analytical and standards support to the DoD Components concerning proper employment of wireless devices.

5.1.7.3. Provide interoperability testing for wireless devices and operational support for spectrum deconfliction and interference resolution.

5.1.7.4. Ensure that wireless capabilities are appropriately integrated into the Defense Information Systems Network.

5.1.7.5. Promote research and development of spectrum-efficient technologies.

5.2. The Under Secretary of Defense for Intelligence, shall:

5.2.1. Ensure that the Director, Defense Intelligence Agency (DIA), provides intelligence support and guidance on the use of wireless technologies for DIA Accredited SCIFs.

5.2.2. Ensure that the Director, Defense Security Service, includes monitoring and assessment of wireless IS security practices and conduct regular inspections of DoD contractors processing classified information in accordance with DoD 5220.22-M (reference (k)).

5.3. The Director, National Security Agency shall:

5.3.1. Implement a capability to assess the risks and vulnerabilities associated with wireless technologies that are responsive to DoD requirements.

5.3.2. Develop and disseminate threat information regarding the capabilities and intentions of adversaries to exploit wireless technologies used by the DoD Components.

5.3.3. Serve as the DoD focal point for Information Security wireless technologies research and development in support of IA requirements to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques. As necessary, coordinate these activities with the Director, Defense Research and Engineering.

5.4. The Chairman of the Joint Chiefs of Staff shall:

5.4.1. Review, confirm, and certify the security and sufficiency of wireless-related interoperability requirements for information systems using wireless capabilities supporting Joint operations.

5.4.2. Develop, coordinate, and promulgate wireless policies and procedures applicable to Joint operations.

5.4.3. Ensure the appropriate review and confirmation of the sufficiency of wireless-related interoperability key performance parameters and information exchange requirements for all capstone requirements documents and operational requirements documents.

5.5. The Commander, U.S. Strategic Command, shall develop defensive actions necessary to detect, deter, or defeat unauthorized wireless activity up to and including computer network attacks against DoD computer networks and to minimize damage from such activities.

5.6. The OSD Principal Staff Assistants shall:

5.6.1. Ensure end-to-end protection and joint interoperability in their functional areas by guiding investments and other actions relating to wireless technologies.

5.6.2. Ensure wireless requirements for information systems and functional applications developed under their cognizance are fully coordinated at the DoD cross-Component level.

5.7. The Heads of the DoD Components shall:

5.7.1. Submit to the DoD CIO, within 120 days of this Directive, specific implementation timelines for compliance of legacy systems to this Directive.

5.7.2. Ensure that all new commercial wireless procurements comply with this Directive immediately. Ensure all entities within their organization and/or under their control that are involved in acquiring (e.g., either developing or procuring) spectrum-dependent (i.e., wireless) systems seek and conform to guidance from the MCEB concerning the licensing and use of wireless systems.

5.7.3. Ensure use of the wireless KM process when evaluating potential wireless solutions.

5.7.4. Ensure that activities evaluating wireless technology provide feedback to the wireless KM process concerning strengths, weaknesses, vulnerabilities, mitigation techniques, and related security procedures.

5.7.5. Acquire PKI-enabled systems in accordance with DoD policy.

5.7.6. Ensure that DAAs, in accordance with the DITSCAP:

5.7.6.1. Control wireless access to IS under their cognizance to ensure that the wireless systems (including external interfaces to commercial wireless services) do not introduce wireless vulnerabilities that undermine the assurance of the other interconnected systems.

5.7.6.2. Include intrusion detection methodologies for the wireless systems.

5.7.6.3. Incorporate wireless topics into annual IA training.

6. EFFECTIVE DATE

This Directive is effective immediately.

Paul Wolfowitz  
Deputy Secretary of Defense

Enclosures - 2

E1. References, continued

E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) [DoD Instruction 5200.40](#), "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 (supplemented by [DoD 8510.1-M](#), "Applications Manual," July 2000)
- (f) Federal Information Processing Standard (FIPS) 140-1, January 11, 1994<sup>2</sup>
- (g) Federal Information Processing Standard (FIPS) 140-2, May 25, 2001<sup>2</sup>
- (h) [DoD Directive 4650.1](#), "Management and Use of the Radio Frequency Spectrum," June 24, 1987
- (i) [DoD Directive 4630.5](#), "Interoperability and Supportability of Information Technology and National Security Systems," January 11, 2002
- (j) [DoD Instruction 4630.8](#), "Procedures for Interoperability and Supportability of Information Technology and National Security Systems," May 2, 2002
- (k) [DoD 5220.22-M](#), "National Industry Security Program Operating Manual," January 1995
- (l) Section 11103 of title 40, United States Code

---

<sup>2</sup> Available via internet at <http://www.itl.nist.gov/fipspubs/>

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1.1. Assured Channel. A network communication link that is protected by a security protocol providing authentication, confidentiality, and data integrity, and employs U.S. Government-approved cryptographic technologies whenever cryptographic means are utilized. The following protocols and mechanisms are sufficient to meet the requirements for an assured channel carrying unclassified data: Internet Protocol Security, Secure Sockets Layer v3, Transport Layer Security, and Secure Multipurpose Internet Mail Extension. Assured channels for classified data must use NSA-approved mechanism to protect the level of classification of the data.

E2.1.2. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

E2.1.3. Commercial Wireless. Devices, Services, and Technologies commercially procured and intended for use in commercial frequency bands.

E2.1.4. Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with Committee on National Security Systems-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

E2.1.5. Designated Approving Authority (DAA). The official authorized to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

E2.1.6. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security.

E2.1.7. End-to-End. IS from the end-user device up to the security border of a DoD network and/or between two user devices connected by a DoD/non-DoD network (to include the wireless infrastructures air interface).

E2.1.8. External Interfaces. Interfaces, including commercial systems (such as a cellular/PCS or pager network not under control of the DAA), capable of carrying traffic between systems under control of the DAA (i.e., the DoD IS and a DoD wireless device).

E2.1.9. Federal Information Processing Standards (FIPS). The standards issued by the National Institute of Standards and Technology for Federal computer systems (<http://www.itl.nist.gov/fipsbubs/>).

E2.1.10. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in 40 U.S.C. 11103 (formerly section 5142 of the Clinger-Cohen Act of 1996) (reference (1)).

E2.1.10.1. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.10.1.1. Transmits information to, receive information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.10.1.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.10.1.3. Processes data or information for use by other equipment, software, and services.

E2.1.10.2. Non-GIG IT -- Stand-alone, self-contained, or embedded IT that is not or shall not be connected to the enterprise network.

E2.1.11. Heads of the DoD Components. For purposes of this policy guidance, the Heads of the DoD Components include: the Office of the Secretary of Defense Principal Staff Assistants, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, the Directors of the Defense Agencies and DoD Field Activities, and the Inspector General of the

Department of Defense, and all other organizational entities in the Department of Defense.

E2.1.12. Identification & Authentication (I&A). Process of accepting a claimed identity and establishing the validity of that claimed identity.

E2.1.13. Information Assurance (IA). Measures used to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.14. Information System (IS). The entire infrastructure, organization, personnel, and components used to collect, process, store, transmit, display, disseminate, and dispose of information.

E2.1.15. Information Technology Systems (ITS). An assembly of computer hardware, software, firmware, or any combination of these, configured to accomplish specific information-handling operations, such as communication, computation, dissemination, processing, and storage of information.

E2.1.16. Personal Digital Assistant (PDA). A generic term for a class of small, easily carried electronic devices used to store and retrieve information.

E2.1.17. Portable Electronic Device (PED). Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDA, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

E2.1.18. Public Key Infrastructure (PKI). That portion of the security management infrastructure dedicated to the management of encryption keys and certificates used by public key-based security services. A PKI is a credentials service; it associates user and entity identities with public keys. A well-run PKI is the foundation on which the trustworthiness of public key-based security mechanisms rests.

E2.1.19. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

E2.1.20. Spectrum Supportability. The expectation, as determined by spectrum management authorities, that a spectrum-dependent system can be provided access to

the electromagnetic spectrum to enable effective system operation. Spectrum supportability incorporates, at a minimum, the spectrum management processes of spectrum certification, designation of frequencies for operation, and electromagnetic compatibility analysis.

E2.1.21. Synchronize. The process of communicating with a host or another PED to upload, download, merge, or swap information (Hot-Synch).

E2.1.22. Wide Area Network (WAN). A system that provides regional, national, or global communication coverage.

E2.1.23. Wireless. Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use IR, acoustic, RF, and optical but, as technology evolves, wireless could include other methods of transmission.

E2.1.24. Wireless Local Area Network (WLAN). A system that provides electromagnetic communication connectivity. Currently it uses either RF or IR technology.

E2.1.25. Wireless Personal Area Network (WPAN). A system that provides electromagnetic communication connectivity over a few yards. Currently it uses either RF or IR technology.